Security Advisory No. 001

Date: 22nd Dec 2021

NicheStack Embedded TCP IP Stack Vulnerabilities (INFRA:HALT)

Advisory ID: PD-2021-0001
Document Version: 1.2
First published: 2021-12-22
Last updated: 2022-11-24, added fixed firmware versions for PDEG, PDEB, DDRC-GRMS-E

Advisory Title

Niche Ethernet stack vulnerabilities can lead to Denial of Service and Breach of Integrity if triggered by specially crafted IP packets.

Summary

Philips Dynalite is aware of multiple vulnerabilities in HCC Embedded's NicheStack TCP/IP third party component, which is integrated into Philips Dynalite's PDEG, PDEB, DDRC-GRMS-E, and DDBC320-Dali v3 (Ethernet).

Security researchers disclosed 14 vulnerabilities in the NicheStack TCP/IP component, of which 8 impact Philips Dynalite's PDEG, PDEB, DDRC-GRMS-E, and DDBC320-Dali v3 (Ethernet) products.

Advisory CVE IDs

CVE ID	CVSSv3.1 base score	Affected protocols	Affected products	Firmware fix info
CVE-2021-31226	9.8	HTTP	PDEG	PDEG 3.57b5
CVE-2021-27565	7.5	HTTP	PDEG	PDEG 3.57b5
CVE-2021-31227	7.5	HTTP	PDEG	PDEG 3.57b5
CVE-2020-35685	9.1	TCP	PDEG, PDEB, DDRC-GRMS-E, DDBC320-Dali v3 (Ethernet)	• PDEG/PDEB 3.57b5 • DDRC-GRMS-E 1.08b1 • DDBC320-Dali v3 - FW release pending
CVE-2021-31400	7.5	TCP	PDEG, PDEB, DDRC-GRMS-E, DDBC320-Dali v3 (Ethernet)	• PDEG/PDEB 3.57b5 • DDRC-GRMS-E 1.08b1 • DDBC320-Dali v3 - FW release pending

CVE-2021-31401	7.5	TCP	PDEG, PDEB, DDRC-GRMS-E, DDBC320-Dali v3 (Ethernet)	• PDEG/PDEB 3.57b5 • DDRC-GRMS-E 1.08b1 • DDBC320-Dali v3 - FW release pending
CVE-2020-35683	7.5	ICMP	PDEG, PDEB, DDRC-GRMS-E, DDBC320-Dali v3 (Ethernet)	• PDEG/PDEB 3.57b5 • DDRC-GRMS-E 1.08b1 • DDBC320-Dali v3 - FW release pending
CVE-2020-35684	7.5	TCP	PDEG, PDEB, DDRC-GRMS-E, DDBC320-Dali v3 (Ethernet)	• PDEG/PDEB 3.57b5 • DDRC-GRMS-E 1.08b1 • DDBC320-Dali v3 - FW release pending

Legend: "FW release pending" = Philips Dynalite will release fixed firmware for this issue. The release date has not been defined yet.

Affected products

PDEG/PDEB	Firmware version 3.55 and prior
DDRC-GRMS-E	Firmware version 1.06 and prior
DDBC320-Dali v3 (Ethernet)	Firmware version 2.03 and prior

Obtaining Software Fixes

Software fixes will be made available through the Philips Dynalite Distributor Support website.

https://www.dynalite.com/support

Mitigations and Workarounds

Customers using the affected devices are strongly recommended to operate the devices in closed networks or protected with a suitable firewall. Use network segmentation to minimize exposure to untrusted networks.

In addition, there are specific workarounds that customers can apply to reduce the risk of exploit:

- For the PDEG, disable the webserver in the device if it is not required, or whitelist HTTP connections. This will mitigate the three HTTP vulnerabilities CVE-2021-31226, CVE-2021-31227, and CVE-2021-27565.
- A properly configured firewall will greatly reduce the risk of malformed TCP and ICMP packets, to mitigate CVE-2021-31400, CVE-2021-31401, and CVE-2020-35684.

Additional Information

The products listed in this advisory are only affected by the subset of vulnerabilities listed here. They are not affected by the other vulnerabilities that are part of the “INFRA:HALT” publication.

More detail and in-depth advice on mitigations can be found in this Forescout blog.

Philips Dynalite supports responsible vulnerability disclosures and encourages researchers and ethical hackers to report identified vulnerabilities. For more information visit our Vulnerability Disclosure page.

Acknowledgements

These vulnerabilities were discovered and reported jointly by Forescout Research Labs and JFrog Security Research. We appreciate the coordinated disclosure of this vulnerability by the finders.

We would also specifically like to thank Dr Elisa Costante and Daniel dos Santos of Forescout for their assistance.

Terms of Use